Guía Rápida de aplicación de la política de firma electrónica de la AGE v1.9

Autor:	*Consejo Superior de Administración Electrónica*
Grupo de trabajo:	*MINETUR-MHAP*
Versión:	*v1.0*
Fecha:	23/06/2014
Fichero:	

ÍNDICE

1 Introducción

La política de firma electrónica y certificados de la Administración General del Estado (AGE) tiene por objeto establecer el conjunto de criterios comunes asumidos por dicha Administración y sus organismos públicos vinculados o dependientes, en relación con la autenticación y la firma electrónica, que afecta a las relaciones de esta Administración con los ciudadanos y entre sus distintos órganos, según lo previsto en el artículo 24.1 del Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

Este documento se circunscribe a los certificados previstos en la Ley 11/2007 expedidos para su empleo por la AGE y los organismos públicos vinculados o dependientes de ésta y a los sistemas de firma electrónica basados en certificados recogidos en el artículo 10.1 y 10.2 del Real Decreto 1671/2009.

En general, una política de firma electrónica es un documento legal que contiene una serie de normas relativas a la firma electrónica, organizadas alrededor de los conceptos de generación y validación de firma, en un contexto particular (contractual, jurídico, legal,…), definiendo las reglas y obligaciones de todos los actores involucrados en dicho proceso.

La política presenta una estructura normalizada del documento electrónico en relación con la creación y validación de firma electrónica, según los estándares técnicos europeos, para facilitar la interoperabilidad de estos documentos, describiendo el alcance y uso de la firma electrónica con la intención de cumplir las condiciones para una transacción concreta en el contexto de las relaciones con los ciudadanos y entre las Administraciones Públicas.

El objetivo de este proceso es determinar la validez de la firma electrónica para una transacción en particular, especificando la información que deberá incluir el firmante en el proceso de generación de la firma, y la información que deberá comprobar el verificador en el proceso de validación de la misma.

2 Alcance de la política de firma

Cuando se firman datos, el firmante indica la aceptación de unas condiciones generales y unas condiciones particulares aplicables a aquella firma electrónica mediante la inclusión de un campo firmado, dentro de la firma, que específica una política. Si el campo correspondiente a la normativa de firma electrónica está ausente y no se identifica ninguna normativa como aplicable, entonces se puede asumir que la firma ha sido generada o verificada sin ninguna restricción normativa, y en consecuencia, que no se le ha asignado ningún significado concreto legal o contractual. Se trataría de una firma que no especifica de forma expresa ninguna semántica o

significación concreta y, por lo tanto, hará falta derivar el significado de la firma a partir del contexto (y especialmente, de la semántica del documento firmado).

Este documento propone una política de firma electrónica, que detalla las condiciones generales para la validación de la firma electrónica y una relación de formatos de objetos binarios y ficheros de referencia que deberán ser admitidos por todas las plataformas implicadas en las relaciones electrónicas de la Administración con los ciudadanos y con las Administraciones Públicas.

Esta política marco es de aplicación a toda la Administración General del Estado, y puede convivir junto con otras políticas particulares para una transacción determinada en un contexto concreto, siempre basadas en dicha política marco.

3 Identificación de la política de firma

Para su identificación univoca, la política de firma dispondrá de un identificador único que podrá ser un OID en ASN.1 o una URI (URL o URN) en XML. Tanto el OID o la URI deberá incluirse obligatoriamente en la firma electrónica, empleando el campo correspondiente para identificar la política marco y la versión con las condiciones generales y específicas de aplicación para su validación, sin perjuicio de lo indicado posteriormente respecto a la posibilidad de acogerse a la modalidad de política implícita.

Se define el identificador de la política de firma de la AGE, con el OID 2.16.724.1.3.1.1.2.x.y, o el urn:oid: 2.16.724.1.3.1.1.2.x.y. Se asignaran identificadores únicos (x.y) para distinguir las versiones sucesivas. En este caso, los valores correspondientes a esta versión son 1.9. También se asignaran identificadores a los distintos formatos de representación (formato legible de PDF, representación en sintaxis XML y representación en sintaxis ASN.1 siguiendo los estándares).

La presente política de firma y las políticas de firmas particulares de cada organismo basadas en esta política marco deberán estar disponibles en formato legible, de modo que puedan ser aplicadas en un contexto concreto para cumplir con los requerimientos de creación y validación de firma electrónica.

Las políticas particulares harán referencia al OID y la URL de la política marco de firma electrónica en la que se inscriben, con indicación expresa de la versión.

Para facilitar el procesado automático de la firma electrónica, la política de firma deberá implementarse a su vez en un formato que pueda ser interpretado y procesado automáticamente por los sistemas encargados de la creación y validación de la firma electrónica.

Las normas técnicas que especifican estas definiciones son:

- ETSI TR 102 038, v.1.1.1. Electronic Signatures and Infrastructures (SEI); XML format for signature policies.

- ETSI TR 102 272, v.1.1.1. Electronic Signatures and Infrastructures (SEI); ASN.1 format for signature policies.

En el caso de la definición de esta versión de la política:

Nombre del documento	**Política de Firma Electrónica y de Certificados de la Administración General del Estado**
Versión	1.9
Identificador de la Política (OID)	2.16.724.1.3.1.1.2.1.9
URL de definición de la política (PDF)	https://sede.060.gob.es/politica_de_firma_anexo_1.pdf
URL de definición de la política (XML)	http://administracionelectronica.gob.es/es/ctt/politicafirma/politica_firma_AGE_v1_9.xml
URL de definición de la política (ASN.1)	http://administracionelectronica.gob.es/es/ctt/politicafirma/politica_firma_AGE_v1_9.dat

4 Formatos admitidos de firma

El formato de los documentos electrónicos con firma electrónica avanzada, aplicada mediante los certificados electrónicos admitidos por las Administraciones Públicas y utilizados en el ámbito de las relaciones con o dentro de la Administración Pública, se deberá ajustar a las especificaciones de los estándares europeos relativos a los formatos de firma electrónica.

El Consejo Superior de la Administración Electrónica será la Entidad gestora encargada de publicar y actualizar la relación de las especificaciones relativas a los formatos admitidos por la presente política de firma.

Actualmente se consideran formatos admitidos:

- formato **XAdES** (XML Advanced Electronic Signatures), según especificación técnica ETSI TS 101 903, versión 1.2.2 y versión 1.3.2.

Asimismo, se admitirá la última versión 1.4.1 a partir del 31-12-2013. Para versiones posteriores del estándar se analizarán los cambios en la sintaxis y se aprobará la adaptación del perfil a la nueva versión del estándar a través de una adenda a esta política de firma.

- formato **CAdES** (CMS Advanced Electronic Signatures), según especificación técnica ETSI TS 101 733, versión 1.6.3 y versión 1.7. Asimismo, se admitirá la última versión 1.8.1 a partir del 31-12-2013. Para versiones posteriores del estándar se analizarán los cambios en la sintaxis y se aprobará la adaptación del perfil a la nueva versión del estándar a través de una adenda a esta política de firma.

- formato **PAdES** (PDF Advanced Electronic Signatures), según especificación técnica ETSI TS 102 778-3, versión 1.2.1 (se admitirán versiones posteriores siempre que no impliquen cambios significativos en la sintaxis de los tags usados en la presente política) y la ETSI TS 102 778-4 para el caso de firmas longevas en PADES (PAdES Long Term). En caso contrario se aprobará la adaptación del perfil a la nueva versión del estándar a través de una adenda a esta política de firma.

  Este formato amplía las especificaciones del estándar de firma en PDF, añadiendo la información adicional de firma similar a la usada en las firmas CAdES o XADES. La parte 3 del estándar PAdES "PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles" recoge la estructura de las firmas PAdES cuando la firma incluida dentro del documento PDF es de tipo CAdES. Su utilización quedará en todo caso limitada a los documentos con formato PDF y que no van a ser tratados en procesos automatizados. Asimismo, se admitirá como formato de intercambio a partir de 31 de diciembre de 2013.

Se tendrá en cuenta la legislación Europea en relación a los formatos de firma admitidos en la Unión Europea, en especial aquellos definidos en los estándares europeos de firma electrónica y por tanto deberá ser actualizada según evolucionen dichas normas Europeas.

Dentro de las distintas clases de los formatos XAdES, CAdES y PAdES, los órganos y unidades administrativas de la Administración Pública deberán adecuar sus sistemas para la generación de, al menos, la clase básica de uno de estos formatos de firma electrónica, añadiendo información sobre la política de firma (clase EPES), y la verificación de las especificaciones de la clase básica de todos estos formatos.

La clase básica de firma electrónica para definir una política de firma electrónica de interoperabilidad es, según los estándares AdES, la clase EPES. A partir de este formato básico EPES es posible incluir suficiente información para validar la firma a largo plazo.

Si fuera necesario generar firmas con validación a largo plazo, se debería implementar un formato que incorporase propiedades adicionales, como información sobre revocación de certificados.

5 Realización de firmas electrónicas - EPES

Para realizar una firma electrónica acorde a una política de firma, es necesario indicarlo en la firma electrónica generada. Para ello, el OID o la URI deberá incluirse obligatoriamente en la firma electrónica, empleando el campo correspondiente, según cada formato, para identificar la política y la versión con las condiciones generales y específicas de aplicación para su validación.

El campo de una firma electrónica *SignaturePolicyIdentifier* identifica la política de firma sobre la que se basa el proceso de generación de firma electrónica.

A continuación se muestran los campos a completar para realizar firmas EPES en los diferentes formatos de firma reconocidos en la política de firma electrónica de la **AGE v1.9**.

Formato	Atributo / Elemento	Valor
CAdES / PAdES	sigPolicyId	2.16.724.1.3.1.1.2.1.9
	sigPolicyHash::hashAlgorithm	1.3.14.3.2.26
	sigPolicyHash::hashValue	G7roucf600+f03r/o0bAOQ6WAs0=
	sigPolicyQualifiers:: sigPolicyQualifierInfo:: sigPolicyQualifierId::SPuri	https://sede.060.gob.es/politica_de_firma_anexo_1.pdf
XAdES	SigPolicyId::Identifier	urn:oid:2.16.724.1.3.1.1.2.1.9
	SigPolicyId::Description	Política de firma electrónica para la Administración General del Estado
	SigPolicyHash::DigestMethod	http://www.w3.org/2000/09/xmldsig#sha1
	SigPolicyHash::DigestValue	G7roucf600+f03r/o0bAOQ6WAs0=
	SigPolicyQualifiers:: SigPolicyQualifier::SPURI	https://sede.060.gob.es/politica_de_firma_anexo_1.pdf

6 Detalle de los formatos de firma admitidos por la política

La política contempla los siguientes estándares europeos de firma electrónica avanzados en su versión básica que permite la implementación de una política de firma:

- **Formato XAdES**, según especificación técnica ETSI TS 101 903, versión 1.2.2 y versión 1.3.2. En este tipo de firmas el fichero de firma es un XML. Los documentos pueden tener cualquier formato. La modalidad de firma que se propone es 'Internally detached', donde genera un único fichero resultante que contiene el

documento original, codificado en base64, y las firmas, encontrándose al mismo nivel XML lo firmado y la firma.

```
<documento>
       <documentoOriginal Id="original" encoding="base64" nombreFichero="orig">
              ...
              ...
              ...
       </documentoOriginal>
       <ds:Signature>
              <ds:SignedInfo/>
                     <ds:Reference URI="#original">
                     </ds:Reference>
              </ds:SignedInfo>
       </ds:Signature>
</documento>
```

Asimismo se admitirán las firmas XAdES enveloped.

- **Formato CAdES**, según especificación técnica `ETSI TS 101 733`, versión 1.6.3 y versión 1.7.4. El fichero de firma es binario. Se adopta el tipo `SignedData` con los datos incluidos (attached/implícito) para la estructura del documento, que mantiene el documento original y la firma en un mismo fichero.

  En el caso de que, debido al tamaño de los datos a firmar, no resulte técnicamente posible o aconsejable realizar las firmas con el formato anteriormente descrito, se generará la estructura de firma detached/explicita, que incluye el hash del documento original en la firma.

- **Formato PAdES**, según especificación técnica `ETSI TS 102 778-3`, versión 1.2.1 y la `ETSI TS 102 778-4` para el caso de las firmas longevas (`PAdES Long Term`). Este tipo de firmas se generarán con la estructura CAdES detached.

7 Datos a incluir en la firma por el firmante

Además de los atributos obligatorios que se especifican en cada uno de los estándares de cada formato, en la firma deberá incluirse como mínimo y de manera obligatoria la siguiente información del firmante:

- **Fecha y hora de firma** (`signingTime`), excepto en el formato PAdES en el que debe indicarse dentro del diccionario `Signature`.
- **Certificado del firmante** (`signingCertificate`)
- **Política de firma** sobre la que se basa el proceso de generación de firma electrónica (`SignaturePolicyIdentifier`).

- **Formato del documento original** que es necesario para que el receptor conozca la forma de visualizar el documento; para XAdES se representará con el atributo `DataObjectFormat`; para CAdES, el atributo es `content-Hints`; para PAdES, no es posible.

Datos opcionales:

- Acción del firmante sobre el documento firmado (lo aprueba, lo informa, lo recibe, lo certifica,...) (`commitmentTypeIndication`).
- Lugar geográfico donde se ha realizado la firma del documento (`signatureProductionPlace` para XAdES y `signer-location` para CAdES); para PAdES en el que debe indicarse dentro del diccionario `Signature`.
- Rol de la persona firmante en la firma electrónica (`signerRole` para XAdES y `signer-attributes` para CAdES/PAdES).
- Sello de tiempo sobre algunos o todos los objetos de la firma (`AllDataObjectsTimeStamp` o `IndividualDataObjectsTimeStamp` para XAdES y `content-time-stamp` para CAdES/PAdES).
- Refrendo de una firma electrónica a través del atributo `CounterSignature`, no permitido en PAdES.
- (Sólo CAdES) Referencia e identificación del documento original (`content-reference` y `content-identifier`).

8 Periodos de gracia para la comprobación del estado de revocación de un certificado.

Para las operaciones de firma, existe un periodo de tiempo de espera, conocido como periodo de precaución o periodo de gracia, para comprobar el estado de revocación de un certificado. Por ello, toda la información de revocación en formatos AdES se recomienda incluirla después de trascurrido el periodo de precaución o periodo de gracia.

Este periodo como mínimo debe ser el tiempo máximo permitido para el refresco completo de las CRLs o el tiempo máximo de actualización del estado del certificado en el servicio OCSP. Estos tiempos podrán ser variables según la Declaración de Prácticas de Certificación del Prestador de Servicios de Certificación.

En la página web de @firma para usuarios registrados de las AAPP, hay una estimación de los periodos de gracia de los PSC que están incorporados en @firma (`http://administracionelectronica.gob.es/es/ctt/afirma`).

9 Inclusión de formatos longevos

Los estándares CAdES (`ETSI TS 101 733`), XAdES (`ETSI TS 101 903`) y PAdES (`ETSI TS 102 778-4`) contemplan la posibilidad de incorporar a las firmas electrónicas información adicional para garantizar la validez de una firma a largo plazo, una vez vencido el período de validez del certificado. Por ello, cada organismo puede extender la firma a partir de la clase EPES a un formato longevo (`AdES –T`, `-C`, `-X`, `-XL`, `-A`) tal y como se detalla a continuación:

1. Sello de tiempo del momento de la firma

- Formato de firma con ello de tiempo EPES –T: Se añade un sello de tiempo (TimeStamp) avalado por una TSA reconocida por el MITyC, con el fin de situar en el tiempo el instante en que se firma un documento.

- El sellado de tiempo debe realizarse en un momento próximo a la fecha incluida en el campo `signingTime` y, en cualquier caso, siempre antes de la caducidad/revocación del certificado del firmante.

2. Formatos longevos (con información de validación)

   En el caso de que se deseen generar firmas longevas, se recomienda incluir la información de validación y añadirle un sello de tiempo a dicha información (formatos EPES–A). En estos tipos de firma la validez de la firma resultante viene determinada por la duración del sello de tiempo que se añade a la firma longeva.

   En el caso que se desee incorporar a la firma la información de validación, se recomienda usar validación mediante OCSP, ya que mediante este método las propiedades o atributos a incluir son de menor tamaño**.**

   Si la consulta al estado de validación de la firma se realiza mediante un método que resulta en una información muy voluminosa (CRL) que aumenta de forma desproporcionada el tamaño de la firma, opcionalmente, en lugar de generar firmas de tipo EPES-A como se ha indicado anteriormente, se pueden incluir referencias a dicha información y un sello de tiempo (formatos EPES-X).

La necesidad de utilizar firmas longevas, o el hecho de utilizar un formato longevo u otro dependerá del procedimiento administrativo concreto, de sus requisitos de

trazabilidad acorde con el ENS (requisito 5.7.5), y de la necesidad de custodia de las firmas durante periodos prolongados de tiempo.

Para determinar la necesidad de usar sellos de tiempo, se puede consultar la guía al respecto:

http://www.seap.minhap.gob.es/dms/es/publicaciones/centro_de_publicaciones_de_la_sgt/Otras_Publicaciones/parrafo/guia_sello_tiempo/Guia_uso_sello_tiempo-INTERNET.pdf

El detalle de la información incluida en los formatos longevos es:

- Formato de firma con información de validación EPES –C: La firma añade un conjunto de referencias a los certificados de la cadena de certificación y su estado (CRL u OCSP).
- Formato de firma extendida EPES –X: Añade sellos de tiempo a las referencias introducidas por AdES –C.
- Formato de firma longeva EPES –XL: Añade los propios certificados y la información de revocación completa para permitir la verificación en el futuro incluso si las fuentes originales no estuvieran ya disponibles.
- Formato de firma de archivo EPES –A: Incluye toda la información necesaria para su verificación en la propia firma y permite la fiabilidad de dicha información mediante sellos de tiempo a lo largo del tiempo. Añade sellos de tiempo a las evidencias introducidas por AdES –XL. El proceso de resellado deberá repetirse antes de que caduque el sello de tiempo.

El sellado de tiempo y la información de validación pueden ser añadidos por el emisor, el receptor o un tercero y se deben incluir como propiedades no firmadas**.**

Conviene señalar que la firma longeva no es el único mecanismo para preservar una firma a lo largo del tiempo. El almacenamiento de los certificados y las informaciones de estado podrá realizarse dentro del documento resultante de la firma electrónica o en un depósito específico:

- en caso de almacenar los certificados y las informaciones de estado dentro de la firma, se recomienda sellar también estas informaciones, siguiendo las modalidades de firmas AdES –X o –A.
- si los certificados y las informaciones de estado se almacenan en un depósito específico, se recomienda sellarlos de forma independiente.

También es posible conservar la validez de las firmas electrónicas mediante la utilización de sistemas de archivo especializados en la custodia. La utilización de dichos sistemas está fuera del alcance de este documento.

Para el archivado y gestión de documentos electrónicos se seguirán las recomendaciones de las guías técnicas de desarrollo del Esquema Nacional de Interoperabilidad (RD 4/2010).

10 Algoritmos criptográficos a usar

Para los entornos de seguridad genérica se tomará la referencia a la URN en la que se publican las funciones de hash y los algoritmos de firma utilizados por las especificaciones XAdES y CAdES, como formatos de firma adoptados, de acuerdo con las especificaciones técnicas ETSI TS 102 176-1 sobre "Electronic Signatures and Infraestructures (ESI); Algorithms and parameters for secure electronic signature". Todo ello sin perjuicio de los criterios que al respecto pudieran adoptarse en el Esquema Nacional de Seguridad, desarrollado a partir del artículo 42 de la Ley 11/2007.

La presente política admite como válidos los algoritmos de generación de hash, codificación en base64, firma, normalización y transformación definidos en los estándares XMLDsig y CMS.

Para los entornos de alta seguridad, de acuerdo con el criterio del Centro Criptológico Nacional, CCN, serán de aplicación las recomendaciones revisadas de la CCN-STIC 405. Asimismo, para garantizar el cumplimiento del Esquema Nacional de Seguridad, se deberá atender a la recomendación CCN-STIC 807 ("Criptografía de Empleo en el ENS").

Se podrán utilizar cualquiera de los siguientes algoritmos para la firma electrónica: RSA/SHA1 (formato que se recomienda reemplazar en el medio plazo por algoritmos más robustos), RSA/SHA256 y RSA/SHA512 que es recomendado para archivado de documentos electrónicos (very long term signatures).

11 Anexo 1: Estructura de la firma electrónica

Este anexo incluye la estructura básica que se deberá seguir para la generación de una firma electrónica:

11.1 Formato de firma electrónica avanzada básico XAdES EPES

```
<ds:Signature ID ? >
     <ds:SignedInfo>
          <ds:CanonicalizationMethod/>
       <ds:SignatureMethod/>
       (<ds:Reference URI ? >
            (<ds:Transforms/>) ?
            <ds:DigestMethod/>
            <ds:DigestValue/>
        </ds:Reference>) +
     </ds:SignedInfo>
     <ds:SignatureValue/>
     (<ds:KeyInfo>) ?
     <ds:Object>
          <QualifyingProperties>
               <SignedProperties>
                 <SignedSignatureProperties>
                      SigningTime
                      SigningCertificate
                      SignaturePolicyIdentifier
                     (SignatureProductionPlace) ?
                     (SignerRole) ?
                 </SignedSignatureProperties>
                 <SignedDataObjectProperties>
                     DataObjectFormat +
                     (CommitmentTypeIndication) *
                     (AllDataObjectsTimeStamp) *
                     (IndividualDataObjectsTimeStamp) *
                    </SignedDataObjectProperties>
               </SignedProperties>
             <UnsignedProperties>
                  <UnsignedSignatureProperties>
                      (CounterSignature) *
                  </UnsignedSignatureProperties>
               </UnsignedProperties>
          </QualifyingProperties>
     </ds:Object>
</ds:Signature>
```

Una firma XAdES-EPES incorpora un elemento firmado incluido dentro de las SignedSignatureProperties llamado **SignaturePolicyIdentifier**. Por tanto, que el elemento sea un subelemento de las propiedades firmadas significa que la información es firmada y aceptada por el firmante. A continuación se define la definición del elemento según el esquema XSD:

```
<xsd:element name="SignaturePolicyIdentifier" type="SignaturePolicyIdentifierType"/>

<xsd:complexType name="SignaturePolicyIdentifierType">
	<xsd:choice>
		<xsd:element name="SignaturePolicyId" type="SignaturePolicyIdType"/>
		<xsd:element name="SignaturePolicyImplied"/>
	</xsd:choice>
</xsd:complexType>

<xsd:complexType name="SignaturePolicyIdType">
	<xsd:sequence>
		<xsd:element name="SigPolicyId" type="ObjectIdentifierType"/>
		<xsd:element ref="ds:Transforms" minOccurs="0"/>
		<xsd:element name="SigPolicyHash" type="DigestAlgAndValueType"/>
		<xsd:element name="SigPolicyQualifiers"      type="SigPolicyQualifiersListType"
		 minOccurs="0"/>
	</xsd:sequence>
</xsd:complexType>

<xsd:complexType name="ObjectIdentifierType">
	<xsd:sequence>
		<xsd:element name="Identifier" type="IdentifierType"/>
		<xsd:element name="Description" type="xsd:string" minOccurs="0"/>
		<xsd:element name="DocumentationReferences" type="DocumentationReferencesType"
		 minOccurs="0"/>
	</xsd:sequence>
</xsd:complexType>

<xsd:complexType name="DigestAlgAndValueType">
	<xsd:sequence>
		<xsd:element ref="ds:DigestMethod"/>
		<xsd:element ref="ds:DigestValue"/>
	</xsd:sequence>
</xsd:complexType>

<xsd:complexType name="SigPolicyQualifiersListType">
	<xsd:sequence>
		<xsd:element name="SigPolicyQualifier" type="AnyType" maxOccurs="unbounded"/>
	</xsd:sequence>
</xsd:complexType>

<xsd:element name="SPURI" type="xsd:anyURI"/>

<xsd:element name="SPUserNotice" type="SPUserNoticeType"/>

<xsd:complexType name="SPUserNoticeType">
	<xsd:sequence>
		<xsd:element name="NoticeRef" type="NoticeReferenceType" minOccurs="0"/>
		<xsd:element name="ExplicitText" type="xsd:string" minOccurs="0"/>
	</xsd:sequence>
</xsd:complexType>

<xsd:complexType name="NoticeReferenceType">
	<xsd:sequence>
		<xsd:element name="Organization" type="xsd:string"/>
		<xsd:element name="NoticeNumbers" type="IntegerListType"/>
	</xsd:sequence>
</xsd:complexType>

<xsd:complexType name="IntegerListType">
	<xsd:sequence>
		<xsd:element name="int" type="xsd:integer" minOccurs="0"
		 maxOccurs="unbounded"/>
	</xsd:sequence>
</xsd:complexType>
```

11.2 Formato de firma electrónica avanzada básico CAdES EPES

Una firma CAdES-EPES incorpora un atributo firmado obligatorio llamado **signaturepolicy-identifier** (1.2.840.113549.1.9.16.2.15), cuyo valor se corresponderá con el OID de la política de firma del Organismo en cuestión. Por tanto, que sea un atributo firmado significa que la información es firmada y aceptada por el firmante. A continuación se define la estructura ASN.1 de dicho atributo:

```
SignaturePolicyIdentifier ::=CHOICE {
        signaturePolicyId SignaturePolicyId,
        signaturePolicyImplied SignaturePolicyImplied -- not used
}

SignaturePolicyId ::= SEQUENCE {
        sigPolicyId SigPolicyId,
        sigPolicyHash SigPolicyHash,
        sigPolicyQualifiers SEQUENCE SIZE (1..MAX) OF SigPolicyQualifierInfo OPTIONAL
}

SigPolicyQualifierInfo ::= SEQUENCE {
        sigPolicyQualifierId SigPolicyQualifierId,
        sigQualifier ANY DEFINED BY sigPolicyQualifierId
}

SigPolicyQualifierId ::= SPuri (1.2.840.113549.1.9.16.5.1)

SPuri ::= IA5String

SigPolicyQualifierId ::= SPUserNotice (1.2.840.113549.1.9.16.5.2)

SPUserNotice ::= SEQUENCE {
        noticeRef NoticeReference OPTIONAL,
        explicitText DisplayText OPTIONAL
}

NoticeReference ::= SEQUENCE {
        organization DisplayText,
        noticeNumbers SEQUENCE OF INTEGER
}

DisplayText ::= CHOICE {
        visibleString VisibleString (SIZE (1..200)),
        bmpString BMPString (SIZE (1..200)),
        utf8String UTF8String (SIZE (1..200))
}

SignaturePolicyImplied ::= NULL
```

12 Anexo 2: Formato de ficheros y objetos binarios admitidos

Este marco de condiciones generales sobre los formatos de fichero de referencia a admitir por las plataformas de relación electrónica de la AGE con los ciudadanos y con las Administraciones Públicas pretende establecer unas consideraciones generales así como la relación de formatos de fichero y objetos binarios que deberán ser admitidos por todas las plataformas para facilitar su interoperabilidad. No obstante lo anterior, estas plataformas podrán admitir otros formatos de acuerdo con las necesidades específicas que en cada caso se planteen.

La relación completa de las condiciones generales en materia de formatos de fichero se establecerá por el marco normativo de desarrollo del Esquema Nacional de Interoperabilidad tal y como estable la Disposición adicional primera del RD 4/2010.

12.1 Consideraciones generales

- Los formatos de los documentos electrónicos admitidos no deberían obligar a disponer de licencias para visualizarlos o imprimirlos en diferentes sistemas operativos. Se deberían evitar en la medida de lo posible los formatos propietarios, porque no es posible asegurar la supervivencia de la empresa. En este sentido, la adhesión a los estándares internacionales es un requisito para la disponibilidad a largo plazo de un documento electrónico.

- Sería deseable disponer de la posibilidad de comprobar automáticamente el formato y su versión antes de admitirlo en el sistema, es decir, sólo se deberían admitir ficheros cuyo formato pudiera ser comprobado por una máquina antes de su aceptación por el Registro electrónico.

- Sólo se deberían admitir formatos estables que gozaran de la aceptación general y tuvieran una expectativa de vida larga. La evolución de los formatos debería mantener compatibilidad con los formatos anteriores.

- Habría que evitar documentos que tuvieran enlaces a otros documentos externos ya que debieran ser autocontenidos. Se considerará como una excepción el caso de los esquemas de validación asociados a formatos XML.

- Debido al riesgo de introducción de código malicioso, se deberá tener especial precaución con aquellos que contengan código ejecutable, como pueden ser macros. La documentación que se presente deberá estar libre de virus informáticos.